What is Claimed is:

1. A method for a sender to send an encrypted message to an authorized recipient, the method having steps comprising:

creating an encrypted content message that may be decrypted using a content decryption key that is unknown to the authorized recipient;

creating an encrypted authentication message that may be decrypted using a recipient's key wherein the recipient's key is known to the authorized recipient but unknown to others except perhaps known to the sender; 112[2]

fixing the encrypted authentication message and the encrypted content message onto a tangible medium and thereafter permitting the authorized recipient to obtain the tangible medium;

if a valid reply has been received, wherein the valid reply is based upon the decrypted authentication message, then allowing the authorized recipient to obtain said content decryption key.

2. The method of claim 1 wherein the recipient's key is a secret key that is shared between the sender and the recipient.

3. The method of claim 1 wherein the recipient's key is a recipient's private key that is associated with a recipient's public key.

4. The method of claim 1 wherein said step of creating an encrypted authentication message further comprises a step of sender authentication encryption such that the authorized recipient may use a sender's key for decryption of the authentication message thereby authenticating that the sender was the source of the encrypted authentication message, such that the sender's key is known to the authorized recipient, and such that the encrypted authentication message may be decrypted with a decryption step employing said recipient's key and with another decryption step employing said sender's key.

5. The method of claim 4 wherein the sender's key is a secret key that is shared between the sender and the authorized recipient but unknown to others.

6. The method of claim 4 wherein the sender's key is a public key that is associated with a sender's private key.

7. The method of claim 1 wherein said step of creating an encrypted content message further comprises a step of sender authentication encryption such that the authorized recipient may use a sender's key for decryption of the encrypted content message thereby authenticating that the sender was the source of the encrypted content message, such that the sender's key is known by the authorized recipient, and such that the encrypted content message may be decrypted by a decryption method with a step employing the recipient's key and with another step employing the sender's key.

8. The method of claim 7 wherein the sender's key is a secret key that is shared between the sender and the authorized recipient but unknown to others.

9. The method of claim 4 wherein the sender's key is a public key that is associated with a sender's private key.

10. An article of manufacture for sending an encrypted message from a sender who possesses a content decryption key to a recipient who possesses a recipient's key, the article, comprising:

a tangible medium;

an encrypted content message fixed on said tangible medium, wherein said encrypted content message may be decrypted using the content decryption key;

an encrypted authentication message fixed on said tangible medium, wherein said encrypted authentication message may be decrypted using the recipient's key;

whereby after the article is delivered to the recipient the recipient may use the recipient's key to decrypt said encrypted authentication message into a decrypted authentication message, the recipient may use the decrypted authentication message to send a valid reply to the sender confirming that the recipient received said article and the sender may then allow the recipient to obtain the content decryption key.

11. The article of claim 10 wherein the recipient's key is a secret key that is shared between the sender and the recipient.

12. The article of claim 10 wherein the recipient's key is a recipient's private key that is associated with a recipient's public key.

13. The article of claim 10 wherein said encrypted authentication message is sender authentication encrypted such that said encrypted authentication message may be decrypted by a decryption method having a step employing the recipient’s key and having another step employing a sender’s key such that the recipient may use the sender’s key to authenticate that the sender was the source of said tangible medium.

14. The article of claim 13 wherein the sender’s key is a secret key that is shared between the sender and the authorized recipient but unknown to others.

15. The article of claim 13 wherein the sender’s key is a public key that is associated with a sender’s private key.

16. The article of claim 10 wherein said encrypted content message is sender authentication encrypted such that said encrypted content message may be decrypted by a decryption method having a step employing the recipient’s key and having another step employing a sender’s key such that the recipient may use the sender’s key to authenticate that the sender was the source of said tangible medium.

17. The article of claim 16 wherein the sender's key is a secret key that is shared between the sender and the authorized recipient but unknown to others.

18. The article of claim 16 wherein the sender's key is a public key that is associated with a sender's private key.

19. A method for an authorized recipient to receive an encrypted message from a sender, the method having steps comprising:

receiving a tangible medium from the sender wherein the tangible medium has fixed upon it an encrypted authentication message and an encrypted content message;

using a recipient's key to decrypt the encrypted authentication message into a decrypted authentication message, wherein the recipient's key is known to the authorized recipient but unknown to others except perhaps known to the sender;

creating a valid reply using the decrypted authentication message;

sending the valid reply to the sender;

if the recipient has received a content decryption key from the sender, then using the content decryption key to decrypt the encrypted content message.